Claims were amended to better claim the invention.

Claim 32 was amended to correct a typographical error.

At Paragraph 3 of the Office Action claim 32 was objected to because it did not end with a period. Amendment of claim 32 is believed to satisfy this objection.

At paragraph 4 of the Office Action claim 34 was rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. It is asserted that: "Data structures must be embodied on a computer readable medium to be statutory."

Claim 34 is:

> 34. Electromagnetic signals propagating on a computer network, comprising: said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of claim 10 or claim 27

Applicant respectfully points out that MPEP 2106 IV, B. 1. (c) (Page 2100-14 of the Eighth Edition) states:

> "Natural Phenomena Such as Electricity and Magnetism.
>
> . . . However, a signal claim directed to a practical application of electromagnetic energy is statutory regardless of its transitory nature."

Applicant respectfully points out that the form of Claim 34 meets the "practical application" requirement of MPEP 2106 IV, B, 1 (c) because the claim is to: "signals carrying instructions for execution on a processor for the practice of the method", and then the method is spelled as that recited in method claims.

Accordingly, Applicant respectfully urges that Claim 34 meets the requirements of 35 U.S.C. § 101 as patentable subject matter, as it explicitly fits in a recited category of patentable subject matter set out in the MPEP.

At Paragraphs 5-6 claims 1 and 10 - 12 were rejected under 35 U.S.C. § 102 as being anticipated by Hawe U. S. Patent 5,070,528 issued December 3, 1991.

The present invention, as set out in representative claim 1 comprises, in part:

> 1. Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:
>
> an encryption execution unit contained within the pipelined processor; and
>
> ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit.***

Hawe discloses a cryptographic processing unit which connects to a MAC interface so that the cryptographic unit can either receive packets as they are received from a network at the MAC interface, or as they stream to the MAC interface for transmission onto the network. The cryptographic unit may be bypassed by a multiplexer if a packet does not require treatment by the cryptographic unit.

Applicant respectfully urges that Haw has no disclosure of a processor controlling a cryptographic unit by the processor issuing opcodes, as claimed in the present invention. That is, Applicant respectfully urges that there is no disclosure in Hawe of Applicant's claimed ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit*** .

Accordingly, Applicant respectfully urges that the Hawe patent is legally precluded from anticipating Applicant's claimed invention under 35 U.S.C. § 102 because of the absence of Applicant's claimed ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit*** .

At Paragraphs 7-8 claims 21-23, 27-29, and 33-34 were rejected under 35 USC 103 as being unpatentable over Hawe in view of Narad et al. U. S. Patent No. 6,157,955.

Narad discloses a network infrastructure which separates classification and action. Narad's overall architecture is shown in his Fig. 3. Some of Narad's timing is shown in his Fig. 14.

Applicant respectfully urges that nowhere does Narad disclose Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit*** .

Accordingly, Applicant respectfully urges that neither Hawe nor Narad, taken either singly or in combination, render the present invention obvious under 35 U.S.C. § 103 because of the absence in both cited patents of Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit*** .

At paragraph 9 of the Office Action claims 21-23, 27-29, and 33-34 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe in view of Johns-Vano et al. U. S. Patent No. 6,026,490 issued February 15, 2000, and Farrell et al. U. S. Patent No. 5,182,800 issued January 26, 1993.

Johns-Vano discloses a cryptographic processing engine which can process two cryptographic algorithms by background staging and algorithm multi-tasking. A three stage pipeline is used.

Farrell discloses a multi-channel direct memory access controller using adaptive pipelining.

Applicant respectfully urges that none of the three cited patents disclose Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit***. That is, in none of the cited patents is there disclosed a processor executing opcodes to control an encryption unit.

Accordingly, Applicant respectfully urges that neither Hawe nor Johns-Vanno nor Farrell taken either singly or in combination, render the present invention obvious under 35 U.S.C. § 103 because of the absence in both cited patents of Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit.***

Accordingly, Applicant respectfully urges that neither Hawe nor Johns-Vanno, nor Farrell, taken either singly or in any combination, render the present invention obvious under 35 U.S.C. § 103 because of the absence in all three cited patents of Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to ef-***

ficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit .

At Paragraph 10 of the Office Action Claims 7-9, 13-14, 16-19, 25-27, and 30-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawe, Narad, Johns-Vano and Farrell.

Applicant respectfully urges that none of the cited patents, Hawe, Narad, Johns-Vano, nor Farrell disclose Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit.*** That is, in none of the cited patents is there disclosed a processor executing opcodes to control an encryption unit.

Accordingly, Applicant respectfully urges that neither Hawe nor Narad nor Johns-Vanno nor Farrell, taken either singly or in any combination, render the present invention obvious under 35 U.S.C. § 103 because of the absence in all four cited patents of Applicant's claimed novel ***a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit .***

At Paragraph 11 of the Office Action claim 20 was rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe in view of Key et al. U. S. Patent No. 6,173,386.

Applicant respectfully points out that under 35 U.S.C. 103 (c) Key is not available as art against the present Application for United States Patent.

At the time that the invention was made, both the Key patent and the present application for United States Patent were both owned by Cisco Technology, Inc.

The assignment of the Key patent is recorded at Reel/Frame 9659/0305, recorded on December 14, 1998, with Cisco Technology, Inc. as assignee by the inventors.

The assignment of the present Application for United States Patent is recorded at Reel/Frame 9664/0560, recorded on December 18, 1998, with Cisco Technology, Inc. as assignee by the inventors.

The statute 35 U.S.C. § 103(c) states:

> "Subject matter developed by another person . . . shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person …."

Accordingly, the provisions of 35 U. S. C. § 103(c) apply, that is Key meets the requirements of the statute, therefore Key cannot preclude patentability of the present Application for United States Patent under 35 U.S.C. § 103(a).

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

A. Sidney Johnston
Reg. No. 29,548
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500

MARK-UP PAGES FOR THE OCTOBER 9, 2002, AMENDMENT TO U.S. PATENT APPLICATION SER. NO. 09/216,519

The replacement for the FIRST full paragraph of page PAGE resulted from the following changes:

COPY PARAGRAPH TO BE AMENDED HERE.

The replacement for claim CLAIM resulted from the following changes:

COPY CLAIM TO BE AMENDED HERE.

1. (Amended) Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:

an encryption execution unit contained within the pipelined processor; and

a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit.

10. (Amended) A method for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the method comprising the steps of:

providing an encryption execution unit within the pipelined processor; and

selectively accessing the encryption execution unit through an integrated hardware and software interface of the pipelined processor that allows efficient cooperation between

the encryption execution unit and resources of the pipelined processor by the pipelined processor executing opcodes to control the encryption execution unit.

20. A programmable processing engine of a network switch comprising:

an input header buffer;

an output header buffer; and

a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked through an integrated hardware and software interface of the microcontroller core to allow efficient cooperation between the encryption TCSM unit and data path resources of the microcontroller core by the microcontroller executing opcodes to control the TCSM.

21. (Amended) A pipelined processor in a network switch, the processor comprising:

an ALU internal to the processor responsive to a first set of opcodes;

an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM) responsive a second set of [encryption] opcodes, and

[wherein] protocol processing operations are performed by the ALU and encryption

operations are performed by the encryption execution unit in response to said second set of opcodes.

27. (Amended) A method for providing encryption functions within a pipelined processor in a network switch, the method comprising the steps of:

associating a first set of opcodes with an ALU internal to the processor;

associating a second set of [encryption] opcodes with an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM), and [wherein] protocol processing operations are performed by the ALU and encryption operations are performed by the encryption execution unit in response to said second set of opcodes.

32. (Amended) The method of Claim 27, further comprising the steps of:

performing a DES function in response to execution of a third instruction having a field containing an encryption opcode that specifies loading plaintext and initialing the DES operations.

32. (Amended) The method of Claim 27, further comprising the steps of:

performing a DES function in response to execution of a third instruction

having a field containing an encryption opcode that specifies loading plaintext and initialing the DES operations[;] .